COMMONWEALTH
OFFICE OF
TECHNOLOGY

COT Security Alert – Microsoft Security Bulletins for January 2012

Microsoft has released seven security bulletins. Microsoft rates one Critical in severity and four Important in severity. Internet Storm Center (ISC) rates three Critical in severity and four as Important.

ISC information may be found at http://isc.sans.org/diary/January+2012+Microsoft+Black+Tuesday+Summary/12361. Microsoft information may be found at the Microsoft Security TechCenter at http://technet.microsoft.com/en-us/security/bulletin/ms12-jan or for each bulletin individually in the links provided below.

MS12-001 Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615) *Important (Security Feature Bypass)*
http://technet.microsoft.com/en-us/security/bulletin/ms12-001

MS12-002 Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381) *Important (Remote Code Execution)* **ISC rated Critical**
http://technet.microsoft.com/en-us/security/bulletin/ms12-002

MS12-003 Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524) *Important (Elevation of Privilege)*
http://technet.microsoft.com/en-us/security/bulletin/ms12-003

MS12-004 Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391) *Critical (Remote Code Execution)* **ISC rated Critical**
http://technet.microsoft.com/en-us/security/bulletin/ms12-004

MS12-005 Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146) *Important (Remote Code Execution)* **ISC rated Critical**
http://technet.microsoft.com/en-us/security/bulletin/ms12-005

MS12-006 Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584) *Important (Information Disclosure)*
http://technet.microsoft.com/en-us/security/bulletin/ms12-006

MS12-007 Vulnerability in AntiXSS Library Could Allow Information Disclosure (2607664) *Important (Information Disclosure)*
http://technet.microsoft.com/en-us/security/bulletin/ms12-007

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Confidentiality Statement - This communication contains information which is confidential. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of distribution, copying, forwarding or use of this communication or the information therein is strictly prohibited and may be unlawful. If you have received this communication in error, please return it to the sender then delete the communication and destroy any copies.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/CISO/